(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－44630

(43)公開日　平成８年(1996)２月16日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ	12/14	３１０　Ｋ			
	12/00	５３７　Ａ	7623－5B		

審査請求　未請求　請求項の数４　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平6－182575

(22)出願日　平成６年(1994)８月３日

(71)出願人　000155469
株式会社野村総合研究所
東京都中央区日本橋１丁目10番１号

(72)発明者　真　下　竜　実
神奈川県横浜市保土ケ谷区神戸町134番地
株式会社野村総合研究所内

(72)発明者　小　野　喜代志
神奈川県横浜市保土ケ谷区神戸町134番地
株式会社野村総合研究所内

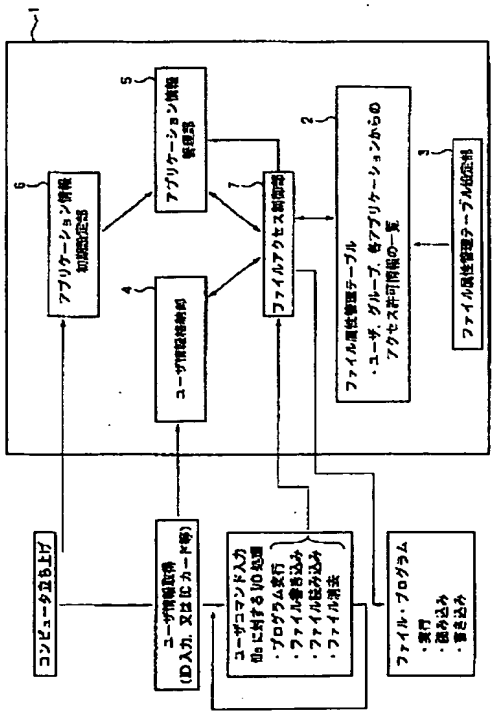
(74)代理人　弁理士　佐藤　一雄　（外３名）

(54)【発明の名称】　ファイルアクセス制御装置およびその制御方法

(57)【要約】

【目的】　複数のアプリケーションソフトウェアからなるソフトウェアの誤作動や不具合あるプログラムの実行による広範なデータ破壊を効果的に防止するファイルアクセス制御装置およびその制御方法を提供する。

【構成】　ファイルごとにそれにアクセスできるユーザとアプリケーションソフトウェアとそのファイルに対する処理の種類を定義したファイル属性管理テーブル２と、ソフトウェアを実行しているユーザの情報を格納するユーザ情報格納手段４と、実行されているアプリケーションソフトウェアの情報を管理するアプリケーション情報管理手段５と、ユーザ情報格納手段４とアプリケーション情報管理手段５とファイル属性管理テーブル２とを参照してファイルに対するアクセス命令を許可あるいは禁止するファイルアクセス制御手段７とを備えた。



1

【特許請求の範囲】
【請求項1】ソフトウェアを構成するファイルごとにそれにアクセスできるユーザとアプリケーションソフトウェアとそのファイルに対する処理の種類を定義したファイル属性管理テーブルと、
前記ソフトウェアを実行中のユーザの情報を格納するユーザ情報格納手段と、
実行中のアプリケーションソフトウェアの情報を管理するアプリケーション情報管理手段と、
前記ファイルに対するアクセス命令が発せられたときに、前記ユーザ情報格納手段と前記アプリケーション情報管理手段とを参照して前記アクセス命令を発したユーザおよびアプリケーションソフトウェアを検出し、前記ファイル属性管理テーブルの定義内容によって前記ファイルに対するアクセス命令を許可あるいは禁止するファイルアクセス制御手段とを備えたことを特徴とするファイルアクセス制御装置。
【請求項2】ファイルごとにこれを読み出し、書き込み、実行および消去できるユーザとアプリケーションソフトウェアとをコンピュータの画面上で設定可能なファイル属性管理テーブル設定手段を備えたことを特徴とする請求項1に記載のファイルアクセス制御装置。
【請求項3】ソフトウェアを構成するファイルごとにこれを読み出し、書き込み、実行および消去することができるユーザとアプリケーションソフトウェアを定義してコンピュータの記憶装置に格納し、
前記ソフトウェアを実行するユーザにユーザ情報を入力させてそのソフトウェアを実行しているユーザとして登録し、
ファイルに対するアクセスの状態を把握することによって、現に実行されているアプリケーションソフトウェアを登録し、
ソフトウェアをファイルに対するアクセス命令が発せられたときに、そのアクセス命令を発したユーザとアプリケーションソフトウェアを検出し、前記ファイルにアクセス可能なユーザとアプリケーションソフトウェアの定義に照らしてそのアクセス命令を許可あるいは禁止することを特徴とするファイルアクセス制御方法。
【請求項4】ソフトウェアが使用される条件に応じて、コンピュータの画面上でソフトウェアを構成するファイルごとにこれを読み出し、書き込み、実行および消去することができるユーザとアプリケーションソフトウェアを定義することを特徴とする請求項3に記載のファイルアクセス制御方法。
【発明の詳細な説明】
【0001】
【産業上の利用分野】本発明は、プログラムやデータのファイルに対するアクセスを制御することにより、誤作動や不正なプログラムの実行によるプログラムやデータの破壊や、ウィルスの感染による大規模なデータ破壊を

2

防止する装置および方法に係り、特にプログラムやデータのファイルごとにこれにアクセス可能なユーザやプログラム（以下、アプリケーションソフトウェアあるいは単にアプリケーションという）を定義し、これによってアプリケーションの連鎖的な実行による大規模なデータ破壊を防止するファイルアクセス制御装置およびその制御方法に関する。
【0002】
【従来の技術】一般にソフトウェアは、一つのソフトウェアの内部に複数のプログラムやデータのファイルを含み、これらプログラム（アプリケーション）を切り替えながら実行してゆくようにしている。
【0003】このようなものとしては、たとえばゲーム用ソフトウェアがある。ゲーム用ソフトウェアでは、最初の画面から次々に新しい画面が展開され、展開された新しい画面ではその画面に沿った動作を行って全体として一つのゲームを楽しめるように構成されている。このような手法はゲーム用ソフトウェアに限らず、現在各種のソフトウェアに広く用いられている。
【0004】上記のようなソフトウェアでは、アプリケーション同士が複雑に関連し合い、一つのアプリケーションが複数の他のアプリケーションによって読み出されあるいは実行されることが可能であり、場合によってはプログラムやデータのファイルが他のアプリケーションによって書き換えあるいは消去されることがある。
【0005】このような構成のソフトウェアでは、オペレーションミスにより、あるいは不具合な部分を有するアプリケーションの実行により、無関係なプログラムやデータのファイル（本来そのアプリケーションの実行によってはアクセスされないファイル）が破壊されたり、さらに連鎖的に無関係なファイルが破壊されたりして、全体的に深刻なデータ破壊を招く危険性があった。
【0006】特に最近問題になっているウィルス感染は、上記現象を意図的に狙ったものであり、データ破壊を隠蔽したプログラムを実行させることにより、連鎖的に広範なデータ破壊を生じさせるものである。
【0007】これに対して従来からアプリケーションによってプログラムやデータのファイルに対するアクセスを制御する装置および方法が提案されていた。この従来のファイルアクセス制御装置および方法は、書き込み不可能なプログラムやデータと書き込み可能なプログラムやデータをそれぞれ、メモリ上のアクセス禁止領域とアクセス許可領域にロードし、アクセス命令の発信源やアクセスする先のプログラムやデータをメモリ上のアドレスによって管理し、これによってファイルに対するアクセスを制御するものであった（特開昭57－71597号公報参照）。
【0008】一方、ユーザによってプログラムやデータのファイルに対するアクセスを許可あるいは禁止する装置および方法が従来からあった。これは、正規の使用を

しようとするユーザにのみファイルに対するアクセス権を与えて、ソフトウェアを保護しようとするものであった。具体的には、ユーザの識別情報を確認することによってユーザ単位で、あるいはユーザグループ単位でファイルに対するアクセスを許可あるいは禁止するものであった。

【0009】

【発明が解決しようとする課題】しかしながら、上記プログラムやデータのファイルをメモリのアクセス可能領域とアクセス禁止領域にロードしてメモリ上のアドレスによって管理する従来の方法では、ソフトウェアの構成に対する制限が多かった。すなわち、複雑なソフトウェアの場合、あるプログラムやデータのファイルは所定のプログラム等からのアクセスに対しては書き込み禁止のファイルとなり、他のプログラム等からのアクセスに対しては書き込み可能なファイルとなるようにきめ細かく構成する必要がある。これに対して、メモリ上の領域によって書き込み可能、書き込み禁止を区別する上記従来の方法では、このような細かい設定を行うことができなかった。

【0010】また、一旦設定した書き込み可能、書き込み禁止の設定をソフトウェアの実行条件によって柔軟に変えることもできなかった。さらに、ユーザによって所定のファイルへのアクセスを許可あるいは禁止することも不可能であった。

【0011】一方、上記ユーザの認証情報を確認することによってアプリケーションに対するアクセスを許可あるいは禁止する従来の方法は、一旦ユーザが正規のユーザと認められれば、そのユーザはそのソフトウェア中のいかなるファイルへのアクセスも可能となる。この結果、正規のユーザの実行命令がオペレーションミスであったり、実行されるプログラムに不具合がある場合には、アプリケーションの連鎖的なデータ破壊を生じることがあった。

【0012】特に、ウィルス感染のソフトウェアは、不具合のあるプログラムを隠蔽し、これを正規のユーザに実行させるので、上記従来の方法では、ウィルスによる広範なデータ破壊を防止することができなかった。

【0013】そこで、本発明の目的は、上記従来の技術の課題を解決し、複数のアプリケーションソフトウェアからなるソフトウェアの誤作動や不具合あるプログラムの実行による広範なデータ破壊を効果的に防止するファイルアクセス制御装置およびその制御方法を提供することにある。

【0014】

【課題を解決するための手段】上記目的達成のために、本願の請求項1に係るファイルアクセス制御装置は、ソフトウェアを構成するファイルごとにそれにアクセスできるユーザとアプリケーションソフトウェアとそのファイルに対する処理の種類を定義したファイル属性管理テーブルと、前記ソフトウェアを実行中のユーザの情報を格納するユーザ情報格納手段と、実行中のアプリケーションソフトウェアの情報を管理するアプリケーション情報管理手段と、前記ファイルに対するアクセス命令が発せられたときに、前記ユーザ情報格納手段と前記アプリケーション情報管理手段とを参照して前記アクセス命令を発したユーザおよびアプリケーションソフトウェアを検出し、前記ファイル属性管理テーブルの定義内容によって前記ファイルに対するアクセス命令を許可あるいは禁止するファイルアクセス制御手段とを備えたことを特徴とするものである。

【0015】本願の請求項2にかかるファイルアクセス制御装置は、上記請求項1のファイルアクセス制御装置において、ファイルごとにこれを読み出し、書き込み、実行および消去できるユーザとアプリケーションソフトウェアとをコンピュータの画面上で設定可能なファイル属性管理テーブル設定手段を備えたことを特徴とするものである。

【0016】本願の請求項3にかかるファイルアクセス制御方法は、ソフトウェアを構成するファイルごとにこれを読み出し、書き込み、実行および消去することができるユーザとアプリケーションソフトウェアを定義してコンピュータの記憶装置に格納し、前記ソフトウェアを実行するユーザにユーザ情報を入力させてそのソフトウェアを実行しているユーザとして登録し、ファイルに対するアクセスの状態を把握することによって、現に実行されているアプリケーションソフトウェアを登録し、ソフトウェアをファイルに対するアクセス命令が発せられたときに、そのアクセス命令を発したユーザとアプリケーションソフトウェアを検出し、前記ファイルにアクセス可能なユーザとアプリケーションソフトウェアの定義に照らしてそのアクセス命令を許可あるいは禁止することを特徴とするものである。

【0017】本願の請求項4に係るファイルアクセス制御方法は、上記請求項3のファイルアクセス制御方法において、ソフトウェアが使用される条件に応じて、コンピュータの画面上でソフトウェアを構成するファイルごとにこれを読み出し、書き込み、実行および消去することができるユーザとアプリケーションソフトウェアを定義することを特徴とするものである。

【0018】

【作用】本願の請求項1および請求項3のファイルアクセス制御装置および制御方法は、ソフトウェアを構成するファイルごとに、それにアクセス可能なユーザとアプリケーションとそのファイルに対する処理の種類を予めファイル属性管理テーブルに定義・登録し、ユーザ情報格納手段にソフトウェアを実行しているユーザの情報を格納し、アプリケーション情報管理手段に現に実行されているアプリケーションソフトウェアの情報を格納し、ファイルに対するアクセス命令があったときに、上記ユ

5

ーザ情報格納手段とアプリケーション情報管理手段からそのアクセス命令を発したユーザとアプリケーションを検出し、上記ファイル属性管理テーブルに照らしてそのアクセス命令を許可あるいは禁止することができる。

【００１９】これにより、上記本発明のファイルアクセス制御装置および制御方法は、ソフトウェアを構成する各ファイルに対してアクセスできるユーザ、アプリケーション、およびそのファイルに対する処理の種類（たとえば、読み出し、書き込み、実行、消去等）を特定でき、ソフトウェアを構成するアプリケーションの正しい作動による処理を保証するとともに、誤作動や不具合なプログラムの実行によるファイルの連鎖的なデータ破壊を防止することができる。

【００２０】また、本願の請求項２および請求項４のファイルアクセス制御装置および制御方法では、コンピュータの画面上でソフトウェアを構成するファイルごとにこれを読み出し、書き込み、実行および消去することができるユーザとアプリケーションソフトウェアを定義することができるので、ソフトウェアが使用される条件に応じて、各ファイルに対するアクセス条件を随時変更することができる。また、このようなファイルに対するアクセス条件を任意に定義できる自由さにより、種々のソフトウェアに対して適用可能なファイルアクセス制御装置および制御方法を得ることができる。

【００２１】

【実施例】以下本発明によるファイルアクセス制御装置及びその制御方法の一実施例について添付の図面を用いて説明する。

【００２２】図１は、本発明によるファイルアクセス制御装置の一実施例の構成とその処理の流れを示している。

【００２３】本実施例のファイルアクセス制御装置１は、ソフトウェアを実行するコンピュータと別のハードウェアによっても構成することができるが、好ましくはソフトウェアによって各ソフトウェアを実行するコンピュータの処理装置、記憶装置、入出力装置等を利用して構成する。

【００２４】図１に示すように、本実施例のファイルアクセス制御装置１は、実行しようとするソフトウェアのファイルごとに、それにアクセスすることができるユーザ、ユーザグループ、アプリケーションソフトウェアを定義したファイル属性管理テーブル２と、前記ファイル属性管理テーブル２の内容を設定するファイル属性管理テーブル設定部３と、現在ソフトウェアを実行しているユーザに関する情報を格納するユーザ情報格納部４と、現在実行中のコマンドがどのアプリケーションソフトウェアのコマンドであるかを把握するアプリケーション情報管理部５と、前記アプリケーション情報管理部５と、前記アプリケーション情報管理部５の初期設定を行うアプリケーション情報初期設定部６と、ファイルに対するアクセス命令があったときに前記ユーザ情報格納部４とアプリケーション情報管理部５とファイル属性管理テーブル２とを参照してファイルに対するアクセスを許可あるいは禁止するファイルアクセス制御部７とからなる。

6

【００２５】次に、上記構成に基づくソフトウェア実行中の上記ファイルアクセス制御装置１の作用について説明する。

【００２６】すでにファイル属性管理テーブル２が設定されているとして、最初にコンピュータを立ち上げた時にアプリケーション情報初期設定部６にコンピュータ起動の信号が入力され、これによってアプリケーション情報が初期状態に設定される。通常、このアプリケーション情報初期設定部６の作用によって、アプリケーション情報管理部５はアプリケーションソフトウェアが何も登録されていない状態に戻される。

【００２７】コンピュータが立ち上がったところで、続いて直にユーザ情報の入力が要求される。これは、ソフトウェアを実行する前に、一次的に不正なユーザを排除するためである。

【００２８】ユーザ情報を取得するには、ユーザにユーザＩＤの入力を求めたり、ＩＣカードによる照合を求める等の公知の方法によって行うことができる。

【００２９】取得されたユーザ情報が正規のユーザのものであるときは、そのユーザによるソフトウェアの使用を許可し、得られたユーザ情報をユーザ情報格納部４に格納する。

【００３０】このようにソフトウェアの使用を許可されたユーザによって、そのソフトウェアが実行されて種々の処理が行われる。これら処理には、ソフトウェアを構成する多数のファイル（プログラムのファイルと、データのファイルとがある）に対する入出力処理も含まれている。

【００３１】本実施例のファイルアクセス制御装置１は、上記ファイルに対する入出力処理の命令は一旦ファイルアクセス制御部７へ入力され、アクセス制御部７によってそのアクセスを許可あるいは禁止する判断が行われ、しかる後に初めてファイルにアクセスできるように構成されている。このファイルに対する入出力処理の種類としては、プログラムの実行、ファイルへの書き込み、ファイルの読み出し、ファイルの消去がある。

【００３２】ファイルアクセス制御部７は、ファイルに対する入出力処理の命令を受け取ったときは、その命令が新しいプログラムを読み込んで実行する命令であるときは、その新しいプログラム名をアプリケーション情報管理部５に登録する。これによって、常に実行中のアプリケーションに関する最新の情報を保持することができる。

【００３３】一方、上記ファイルに対する入出力処理の命令が所定のファイルの内容を変更または消去する命令であるときは、ファイルアクセス制御部７は、ユーザ情

報格納部４とアプリケーション情報管理部５とファイル属性管理テーブル２の内容を参照し、その命令が、対象となっているファイルに対してアクセスする権限を与えられているユーザおよびアプリケーションソフトの命令であるか否か、また、その命令による処理の種類が許可されているものであるか否かを判断し、その命令を実行を許可あるいは禁止する。

【００３４】次に上記判断の基準となるファイル属性管理テーブルの内容について説明する。

【００３５】図２は、ファイル属性管理テーブル設定部３によるファイル属性管理テーブル２の内容設定の画面の一例を示している。

【００３６】図２において、画面の上部は設定画面の検索条件を設定する部分であり、ファイル名、ユーザ名、ユーザグループ名、タイプ、ファイルＩＤの少なくとも１つを入力することにより、ファイル属性管理テーブル設定部３は、その検索条件に合致したファイルのファイル属性管理テーブルの設定画面を表示する。

【００３７】上記設定画面検索条件を入力する部分の下方がファイル属性管理テーブルの内容を設定する画面である。

【００３８】ファイル属性管理テーブルの内容を設定する画面の左側部分は、アクセスの対象となるファイルの名称（ここではmain.exe、image.dat 、sub.exe 、hiscore.dat ）、アクセスを行なうユーザ（α）、ユーザグループ（β）、各ファイルに付与されるアプリケーションとしてのＩＤ（ＸＸＸ）を設定する画面となっている。

【００３９】上記ファイル、ユーザ等を設定する画面の右側には、各ファイルに対するアプリケーションのアクセス条件を設定する画面となっている。このアクセス条件設定画面は、大きくユーザ管理の設定画面とアプリケーション管理の設定画面に分けられている。

【００４０】ユーザ管理の設定画面は、ユーザとユーザグループとユーザおよびユーザグループ以外のアクセス許可条件に分けられている。この区分けは例示であり、必要に応じてさらに細かい指定、たとえば各ユーザごとのアクセス許可条件を設定することもできる。

【００４１】このユーザ管理の区分け欄の下方には、対象となるファイルに対する処理の種類（読み出し、書き込み、実行、消去）ごとに許可あるいは禁止する条件を設定する画面が表示されている。

【００４２】同様に、アプリケーション管理の設定画面は、同一のアプリケーションＩＤからのアクセスと、異なるアプリケーションＩＤからのアクセスとに分けられ、それぞれのアプリケーションからのアクセスに対してその処理の種類ごとに許可あるいは禁止の条件を設定できるようになっている。ここでも、必要に応じてさらに細かい指定、例えばアプリケーションＩＤごとのアクセス条件を設定することができる。

【００４３】図２の設定例では、ファイルmain.exeは、ユーザ・ユーザグループ以外の人は読み出しのみでき、正規のユーザαとユーザグループβは実行することができる。さらにユーザαは、ファイルmain.exeを書き換えあるいは消去することができる。また、ファイルmain.exeは、全ての他のアプリケーション・ソフトウェアによって起動および実行されることが可能である。

【００４４】これに対してファイルimage.dat は、同一ＩＤのアプリケーションのみによって参照および書き換えられ、しかもユーザαのみが書き換えを行なうことができる。

【００４５】また、ファイルsub.exe は、ユーザαとユーザグループβの人によって、main.exe（同一ＩＤ）を通じてのみ実行される。ユーザαは、ファイルsub.exeを消去できるが、誤操作防止のために書き換えを行なうことはできない。

【００４６】最後にファイルhiscore.dat は、ユーザαとユーザグループβの人がファイルmain.exeまたはsub.exe を通じてのみ参照および書き換えを行うことができる。また、消去することができるのはユーザαのみである。

【００４７】このように本発明は、ファイル属性管理テーブル２のユーザ管理、アプリケーション管理および許可する処理の種類を設定することにより、ファイルごとにこれにアクセスできるユーザとアプリケーションと処理の種類を自由に設定することができる。また、上記ファイル属性管理テーブル２の設定は、ファイル属性管理テーブル設定部３によって必要な時に行うことができるので、ソフトウェアの実行条件、たとえばファイルにアクセスできるユーザを追加・変更したり、ソフトウェアの設計仕様の変更によって各ファイルにアクセスできるアプリケーションを追加・変更するができる。また、上記ファイルに対するアクセス条件の自由な設定により、本発明のファイルアクセス制御装置および制御方法は種々のソフトウェアに適用可能な汎用性が高いものとなる。

【００４８】次にファイルアクセス制御部７におけるアクセス制御を具体的なアプリケーションの動作に沿って説明する。

【００４９】図３はファイルアクセス制御部７による制御の一例を時系列的に示したものである。図３で例示するソフトウェアは、複数のアプリケーションソフトを含み、これらのアプリケーションソフトがユーザのコマンドによって一定の手順で次々に起動および実行されるように構成されているものとする。

【００５０】図３ではメインのアプリケーションＰＲＧ－Ａが起動され、このメインのアプリケーションＰＲＧ－ＡによってファイルＦＬＬＥ－Ａが書き換えられる場合が示されている。

【００５１】この場合、前記ファイル属性管理テーブル

2には、ユーザαは直接メイン・アプリケーションPRG－Aを起動でき、メイン・アプリケーションPRG－Aを通じてサブ・アプリケーションPRG－Bを起動でき、サブ・アプリケーションPRG－Bを通じてはデータファイルFILE－Aを書き換えられるように予め設定しておくものとする。

【0052】図3において、コンピュータの立ち上げ後ユーザIDαが獲得されたとすると、このユーザIDαは正規ユーザのものであるか否かを判断され、正規ユーザのものである場合はユーザ情報格納部4に格納される（ステップ100）。

【0053】格納されたユーザIDαは新たなユーザIDが獲得されない限り、すなわち、ソフトウェアを中止して再度コンピュータを立ち上げない限り有効に存続する。

【0054】なお、図3には示していないが、図1で説明したように、コンピュータの立ち上げ時に、アプリケーション情報管理部5は初期状態、すなわち何も登録されていない状態に戻される。

【0055】次にメイン・アプリケーションPRG－Aを実行するコマンドを入力したとすると、このPRG－Aに対するアクセスの情報がファイルアクセス制御部7によって検知され、ファイルアクセス制御部7は、PRG－Aを実行しようとするユーザとアプリケーションをそれぞれユーザ情報格納部4とアプリケーション情報管理部5によって検出する（ステップ110）。

【0056】この場合は、ユーザ情報格納部4からはユーザ情報αを得るものの、アプリケーション情報管理部5が未登録の状態であるので、ユーザαによる直接のPRG－Aの読み出し命令であることがわかる。ここでは、ユーザαによるメイン・アプリケーションPRG－Aの直接の読み出しは可能なように前記ファイル属性管理テーブル2に定義されているので、メイン・アプリケーションPRG－Aは実行され、同時に現在実行中のアプリケーションがPRG－Aであることがアプリケーション情報管理部5に登録される（ステップ120）。

【0057】上記アプリケーション情報管理部5に登録されたアプリケーション情報（PRG－A）は、PRG－Aの実行が終了するまでアプリケーション情報管理部5に有効に存続する。

【0058】次にソフトウェア実行中にPRG－Aによってサブ・アプリケーションPRG－Bの実行命令が発せられたとする。このサブ・アプリケーションPRG－Bに対するアクセス命令はファイルアクセス制御部7によって検知され、ファイルアクセス制御部7はサブ・アプリケーションPRG－Bに対する実行命令の発信源であるユーザとアプリケーションをユーザ情報格納部4とアプリケーション情報管理部5に問い合わせる（ステップ130）。

【0059】この結果、このPRG－Bの実行命令は、

ユーザαがメイン・アプリケーションPRG－Aを通じて行っているものとわかり、ファイルアクセス制御部7はファイル属性管理テーブル2の設定条件に基づいてサブ・アプリケーションPRG－Bの実行命令を許可する。

【0060】サブ・アプリケーションPRG－Bが実行されると、ファイルアクセス制御部7は現在実行中のアプリケーションがサブ・アプリケーションPRG－Bであることをアプリケーション情報管理部5に追加登録する（ステップ140）。

【0061】次に、サブ・アプリケーションPRG－Bの実行によって、データファイルFILE－Aに対する書き込み命令が発せられたとする。ファイルアクセス制御部7は、このデータファイルFILE－Aに対する書き込み命令を発したユーザとアプリケーションをユーザ情報格納部4とアプリケーション情報管理部5へ問い合わせる。この結果、ユーザαがサブ・アプリケーションPRG－Bを通じてデータファイルFILE－Aの内容を書き換えるものであると判断し、ファイル属性管理テーブル2の設定条件によってこの書き込み命令を禁止する（ステップ150）。

【0062】続いてサブ・アプリケーションPRG－Bの実行が終了した場合について説明する。サブ・アプリケーションPRG－Bの実行が終了すると、ファイルアクセス制御部7はこれを検知し、アプリケーション情報管理部5に登録されていたサブ・アプリケーションPRG－Bを消去する（ステップ160）。

【0063】サブ・アプリケーションPRG－Bの実行が終了すると、中断されていたメイン・アプリケーションPRG－Aが実行され、さらに、この状態でメイン・アプリケーションPRG－Aの実行によってデータファイルFILE－Aに対する書き込み命令が発せられたとする。この場合は、ファイルアクセス制御部7はユーザαかメイン・アプリケーションPRG－Aを通じてデータファイルFILE－Aを書き換えようとしたものと判断し、ファイル属性管理部2の設定条件によってデータファイルFILE－Aの書き換えを許可する（ステップ170）。

【0064】図4および図5は本発明によるファイルアクセス制御装置および制御方法による制御のパターンを例示したものである。

【0065】図4はユーザ管理を中心に、所定のユーザXが特定のプログラムAの動作によってのみファイル1を更新／消去できるように制御する場合を示している。

【0066】図4（a）は、ユーザXかプログラムAを通じて行うファイル処理を示しており、読み出し、書き込み、消去、実行のいずれも行うことができる。

【0067】これに対して、図4（b）はユーザXが指定以外のプログラムBを通じて行うファイル処理を示しており、この場合は、誤作動によるデータ破壊を防止す

るために読み出しのみ可能である。

【００６８】図４（ｃ）は、ユーザＸ以外のユーザ（Ｙ）が行うことができるファイル処理を示しているが、この場合は、たとえプログラムＡによっても読み出しのみが可能となる。

【００６９】図５は、アプリケーション管理を中心として、特定のプログラムＢの動作のみによってのみファイル２を実行可能とする制御を行う場合を示している。

【００７０】図５（ａ）はいかなるユーザＸ、Ｙであっても、プログラムＢを通じてのみファイル２を読み出し、実行できることを示している。これに対して図５（ｂ）に示すように、いかなるユーザＸ、ＹであってもプログラムＡを通じては、ファイル２を読み出し、書き込み、消去、実行できないことを示している。

【００７１】このように、ユーザ管理を中心するファイルに対するアクセスと、アプリケーション管理を中心とするファイルに対するアクセスとを組み合わせることにより、種々のファイルアクセスの制御を行うことができ、これによってソフトウェアを構成するアプリケーション間の関係をきめ細かく規定することができる。

【００７２】これにより、たとえば、不具合な部分を有するプログラムを誤って実行したような場合、その不具合があるプログラムによるデータ破壊は、ごく限られたファイルにのみ及ぶ。この結果、アプリケーションソフトウェアの誤作動や不具合があるプログラムやウィルス感染による広範なデータ破壊を実質的に防止することができる。

【００７３】

【発明の効果】上記説明から明らかなように、本願請求項１および請求項３に係るファイルアクセス制御装置および制御方法は、ファイル属性管理テーブルと、アプリケーション情報管理手段と、ユーザ情報格納手段と、ファイルアクセス制御手段の作用により、所定のファイルに対してアクセスできるユーザとアプリケーションを制限し、かつ、そのユーザとアプリケーションによるファイルの処理を特定の種類に制限することができるので、無関係なプログラム（アプリケーション）の実行によってファイルが書き換えあるいは消去されることを防止でき、これによって、誤作動や不具合のあるプログラムの実行やウィルス感染等による広範かつ深刻なデータ破壊を実質的に防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施例によるファイルアクセス制御装置の構成と、その構成部分間の情報の流れを概略示した図。

【図２】本発明のファイル属性管理テーブルの設定画面の一例を示した図。

【図３】具体的なアプリケーションを用いて本発明のファイルアクセス制御部の動作を時系列的に示した流れ図。

【図４】ユーザ管理を中心とする所定のファイルに対するアクセスの態様を示した図。

【図５】アプリケーションソフトウェア管理を中心とする所定のファイルに対するアクセスの態様を示した図。

【符号の説明】

１　ファイルアクセス制御装置
２　ファイル属性管理テーブル
３　ファイル属性管理テーブル設定部
４　ユーザ情報格納部
５　アプリケーション情報管理部
６　アプリケーション情報初期設定部
７　ファイルアクセス制御部

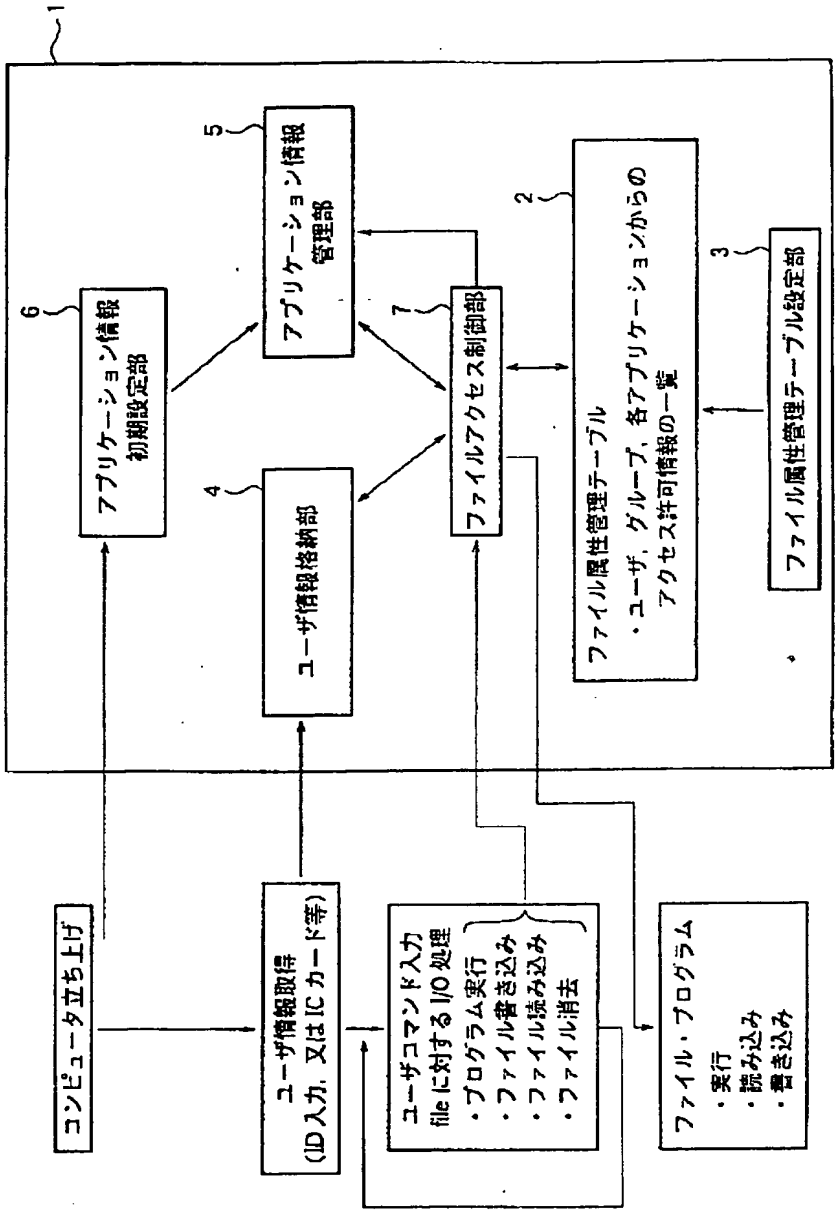
【図２】

設定画面検索条件

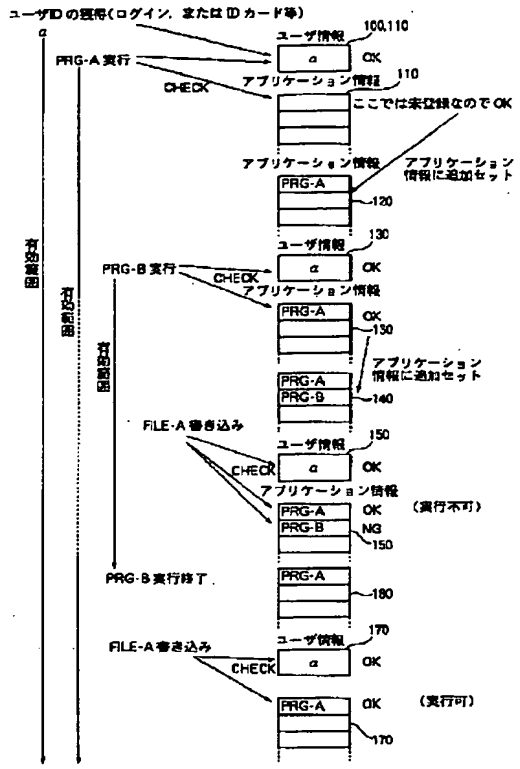
ファイル名＿＿＿＿ユーザ名＿＿＿＿ユーザグループ名＿＿タイプ＿＿アプリケーションID＿＿＿

				ユーザ管理			アプリケーション管理	
				ユーザ	ユーザグループ	ユーザ・ユーザグループ外	同一ID	同一ID外
名称	ユーザ	ユーザグループ	アプリケーションID	読書実消	読書実消	読書実消	読書実消	読書実消
main.exe	α	β	XXX	☑☑☑☑	☑☑☐	☑☐☐	☑☑☐	☑☑☐
image.dat	α	β	XXX	☑☑☐☑	☑☐☐☐	☑☐☐☐	☑☑☐☐	☑☐☐☐
sub.exe	α	β	XXX	☑☐☑☑	☑☑☐☐	☑☐☐☐	☑☑☐☐	☑☐☐☐
Hiscore.dat	α	β	XXX	☑☑☐☑	☑☑☐☐	☑☐☐☐	☑☑☐☐	☑☐☐☐

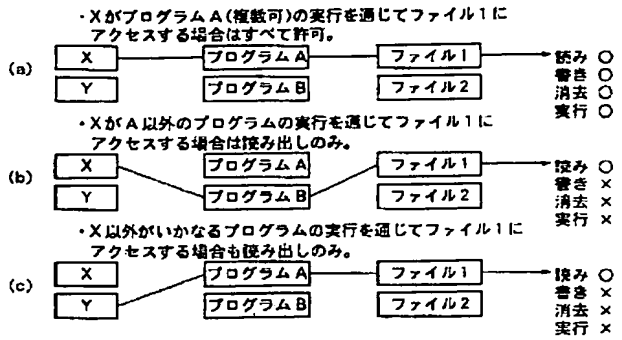
【図1】


1
5
アプリケーション情報
管理部
2
ファイル属性管理テーブル
・ユーザ，グループ，各アプリケーションからの
アクセス許可情報の一覧
3
ファイル属性管理テーブル設定部
6
アプリケーション情報
初期設定部
4
ユーザ情報格納部
7
ファイルアクセス制御部
コンピュータ立ち上げ
ユーザ情報取得
(ID入力，又はICカード等)
ユーザコマンド入力
fileに対するI/O処理
・プログラム実行
・ファイル書き込み
・ファイル読み込み
・ファイル消去
ファイル・プログラム
・実行
・読み込み
・書き込み

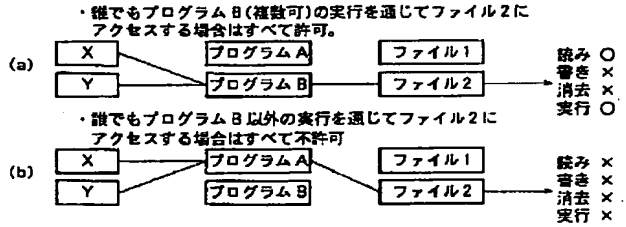
【図3】


ユーザIDの要求(ログイン, またはIDカード等)
α
ユーザ情報
100,110
α
OK
PRG-A実行
CHECK
アプリケーション情報
110
ここでは未登録なのでOK
アプリケーション情報
PRG-A
120
アプリケーション情報に追加セット
ユーザ情報
130
PRG-B実行
CHECK
アプリケーション情報
PRG-A
OK
130
PRG-A
PRG-B
140
アプリケーション情報に追加セット
FILE-A書き込み
ユーザ情報
150
CHECK
アプリケーション情報
PRG-A
OK
(実行不可)
PRG-B
NG
150
PRG-B実行終了
PRG-A
180
FILE-A書き込み
ユーザ情報
170
CHECK
OK
PRG-A
OK
(実行可)
170
有効範囲
有効範囲
有効範囲

【図4】


・XがプログラムA(複数可)の実行を通じてファイル1にアクセスする場合はすべて許可。
(a)
X
Y
プログラムA
プログラムB
ファイル1
ファイル2
読み ○
書き ○
消去 ○
実行 ○
・XがA以外のプログラムの実行を通じてファイル1にアクセスする場合は読み出しのみ。
(b)
X
Y
プログラムA
プログラムB
ファイル1
ファイル2
読み ○
書き ×
消去 ×
実行 ×
・X以外がいかなるプログラムの実行を通じてファイル1にアクセスする場合も読み出しのみ。
(c)
X
Y
プログラムA
プログラムB
ファイル1
ファイル2
読み ○
書き ×
消去 ×
実行 ×

【図5】


・誰でもプログラムB(複数可)の実行を通じてファイル2にアクセスする場合はすべて許可。
(a)
X
Y
プログラムA
プログラムB
ファイル1
ファイル2
読み ○
書き ×
消去 ×
実行 ○
・誰でもプログラムB以外の実行を通じてファイル2にアクセスする場合はすべて不許可
(b)
X
Y
プログラムA
プログラムB
ファイル1
ファイル2
読み ×
書き ×
消去 ×
実行 ×